Exhibit 2

EVIDENCE OF USE FOR U.S. PATENT NO. US6236983

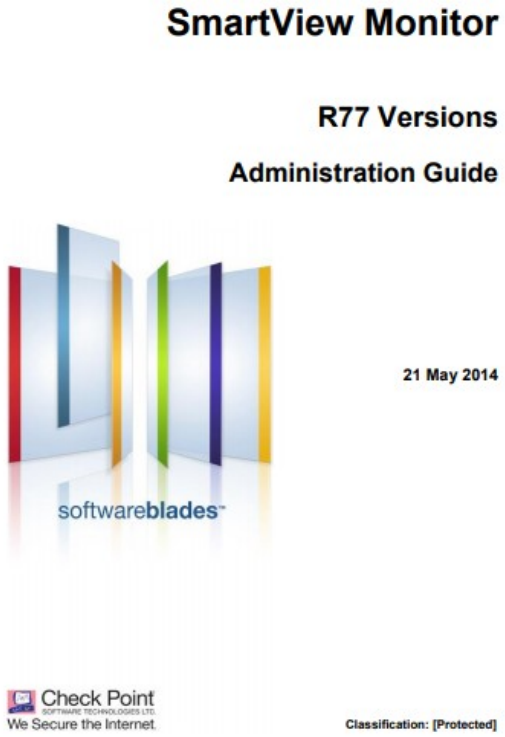
Title: Method and apparatus for collecting information regarding a device or a user of a device

Application No.: 09/017,112

Filing Date: 1998-01-31

Issue Date: 2001-05-22

Accused Product/Standard:



Source: http://supportcontent.checkpoint.com/documentation_download?ID=24848

Check Point
SOFTWARE TECHNOLOGIES LTD.

Check Point R7X, R80.X and R81 Upgrade Map

		Target Release								
	Major Release	**R77**				**R80**	**R80.20**			**R81**
	Minor Release	R77	R77.10	R77.20	R77.30	R80.10	R80.20	R80.30	R80.40	R81
	Release Date	Sep 2013	Jan 2014	July 2014	May 2015	May 2017	Sep 2018	May 2019	Jan 2020	Oct 2020
	End-of-Support	Support Ended Sep 2019				Jan 2022	September 2022			Oct 2024
Currently Installed	**R77** R77		√	√	√	√	√	√	√	
	R77 R77.10			√	√	√	√	√	√	
	R77 R77.20				√	√	√	√	√	
	R77 R77.30					√	√	√	√	√**
	R80 R80*					√	√	√	√	√**
	R80 R80.10						√	√	√	√**
	R80.20 R80.20 M1*						√	√	√	√
	R80.20 R80.20							√	√	√
	R80.20 R80.20 M2*							√	√	√
	R80.20 R80.30								√	√
	R80.20 R80.40									√

Note:

√ * - R80, R80.20.Mx are Management Versions only

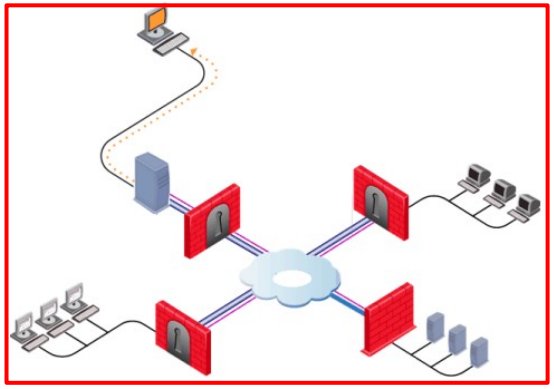
√ ** - For Security Management, first upgrade to R80.40

For exceptions, limitations and instructions please carefully read Check Point Release Notes before upgrading

Supported Check Point Major Releases:
R80
R80.20
R81

Source: https://downloads.checkpoint.com/dc/download.htm?ID=18761

Evidence of Use

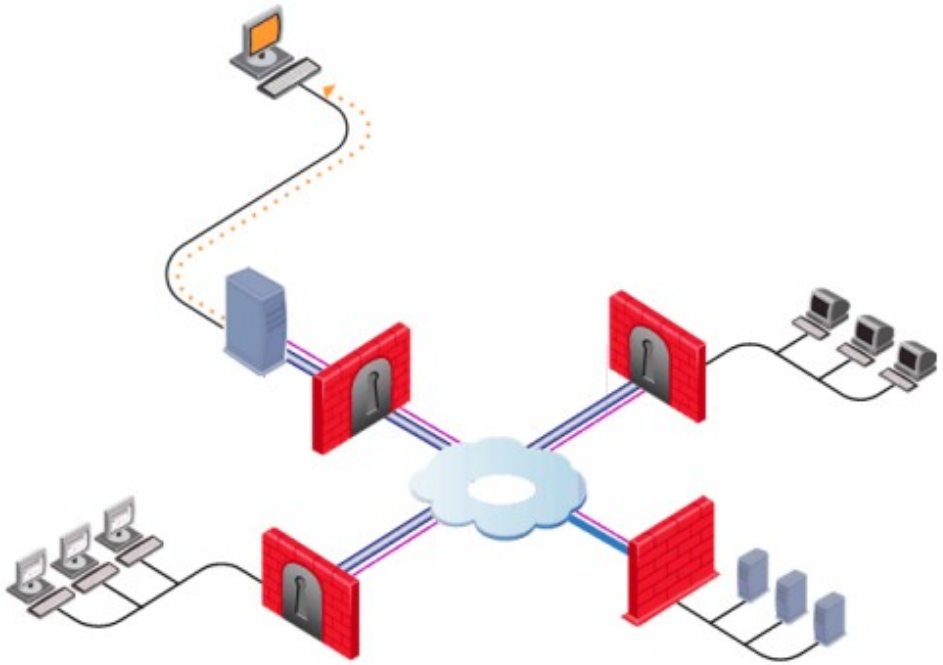
Claim Language	Evidence of Infringement
1. In a computer system, a method of collecting information, the method comprising:	Check Point's SmartView Monitor provides a method of collecting information in a computer system. Security Management Server collects status information for all the components in the system. **How SmartView Monitor Works** Data for the status of all gateways in the system is collected by the Security Management Server and viewed in SmartView Monitor. The data shows status for: • Check Point Security Gateways • OPSEC gateways • Check Point Software Blades Gateway Status is the SmartView Monitor view that displays all component status information. A Gateway Status view displays a snapshot of all Software Blades, such as VPN and ClusterXL, as well as third party products (for example, OPSEC-partner gateways).  Source: http://supportcontent.checkpoint.com/documentation_download?ID=24848, Page 17 of 44

Claim Language	Evidence of Infringement
receiving information from a discovery agent, wherein the discovery agent collects information about the computer system or a user, when the discovery agent is activated;	The Security Management server receives information from a gateway (i.e., "discovery agent") and may be viewed on the SmartView Monitor. The gateways collect status information for the components in the system. For example, the collected information may include the status or nature of connections to the gateway(s), suspicious activity observed by the gateway, etc. The Check Point gateway (i.e., "discovery agent") is activated when the SIC (Secure Internal Communications) has been initialized. Therefore, the information is gathered when the Check Point gateway is initialized or activated. **How SmartView Monitor Works** Data for the status of all gateways in the system is collected by the Security Management Server and viewed in SmartView Monitor. The data shows status for: • Check Point Security Gateways • OPSEC gateways • Check Point Software Blades Gateway Status is the SmartView Monitor view that displays all component status information. A Gateway Status view displays a snapshot of all Software Blades, such as VPN and ClusterXL, as well as third party products (for example, OPSEC-partner gateways). ***The Need for Suspicious Activity Rules*** The connection of enterprise and public networks is a great information security challenge, since connections that provide access to employees and customers can also act as an open doorway for those who want to attack the network and its applications. Modern business needs require that information be easily accessed while at the same time it remains secure and private. The fast changing network environment demands the ability to immediately react to a security problem without having to change the entire network's Firewall rule base (for example, you want to instantly block a specific user). All inbound and outbound network activity should be inspected and identified as suspicious when necessary (for instance, when network or system activity indicates that someone is attempting to break in).

Claim Language	Evidence of Infringement
	AMON The Security Management Server acts as an AMON client. It collects data about installed Software Blades. Each Security Gateway, or any other OPSEC gateway which runs an AMON server, acts as the AMON server itself. The gateway requests status updates from other components, such as the Firewall kernel and network servers. Requests are fetched at a defined interval. An alternate source for status collection can be any AMON client, such as an OPSEC partner, which uses the AMON protocol. The AMON protocol is SIC- based. It can collect data only after SIC is initialized. Source: http://supportcontent.checkpoint.com/documentation_download?ID=24848, Pages 17, 15 and 18 of 44

Claim Language	Evidence of Infringement
determining one or more of a plurality of discovery rules to be applied to the information received from the discovery agent; and	The Suspicious Activity Rules are rules that are integrated into SmartView Monitor. These rules are applied upon the detection of suspicious network activity by the gateways. The Suspicious Activity Rule that is applied depends upon the suspicious activity detected by the gateway. Therefore, the Check Point's SmartView Monitor determines one or more of a plurality of discovery rules to be applied to the information received from the discovery agent. ***Suspicious Activity Rules*** Suspicious Activity Monitoring (SAM) is a utility integrated in SmartView Monitor. It blocks activities that you see in the SmartView Monitor results and that appear to be suspicious. For example, you can block a user who tries several times to gain unauthorized access to a network or Internet resource. A Security Gateway with SAM enabled has Firewall rules to block suspicious connections that are not restricted by the security policy. These rules are applied immediately (**Install Policy** not required). **To define SmartView Monitor actions on rule match:** 1. In the **Block Suspicious Activity** window, click **Advanced**. The **Advanced** window opens. 2. In **Action**, select the Firewall action for SmartView Monitor to do on rule match: ▪ **Notify** - Send a message about the activity, but do not block it. ▪ **Drop** - Drop packets without sending a response. The connection will eventually time out. ▪ **Reject** - Send an RST packet to the source and close the connection. Source: http://supportcontent.checkpoint.com/documentation_download?ID=24848, Pages 15 and 16 of 44

Claim Language	Evidence of Infringement
applying the one or more discovery rules to the information received from the discovery agent, wherein the discovery agent and the discovery rule are separate code sequences located in the computer system.	The SmartView Monitor is integrated with Suspicious Activity Monitoring (SAM) that enables actions to be performed based on the received information of suspicious activity provided to the SmartView Monitor by the gateways. The defined actions are taken (e.g., Notify, Drop, Reject) when a particular Suspicious Activity Rule is triggered and applied. The code sequence responsible for collecting and sending the alert regarding the suspicious activity is located on the gateway(s). The suspicious activity rules are located/integrated in the SmartView Monitor. Therefore, the code sequence responsible for the collecting and sending to the SmartView Monitor of suspicious activity on the gateway is separate from the code sequence of the suspicious rules. ***Suspicious Activity Rules*** Suspicious Activity Monitoring (SAM) is a utility integrated in SmartView Monitor. It blocks activities that you see in the SmartView Monitor results and that appear to be suspicious. For example, you can block a user who tries several times to gain unauthorized access to a network or Internet resource. A Security Gateway with SAM enabled has Firewall rules to block suspicious connections that are not restricted by the security policy. These rules are applied immediately (**Install Policy** not required). **To define SmartView Monitor actions on rule match:** 1. In the **Block Suspicious Activity** window, click **Advanced**. The **Advanced** window opens. 2. In **Action**, select the Firewall action for SmartView Monitor to do on rule match: ▪ **Notify** - Send a message about the activity, but do not block it. ▪ **Drop** - Drop packets without sending a response. The connection will eventually time out. ▪ **Reject** - Send an RST packet to the source and close the connection.

Claim Language	Evidence of Infringement
	 SIC is initialized between Security Gateways (local and remote) and the Security Management Server. The Security Management Server then gets status data from the Software Blades with the **AMON** (Application Monitoring) protocol. SmartView Monitor gets the data from the Security Management Server. Source: http://supportcontent.checkpoint.com/documentation_download?ID=24848, Pages 15, 16 and 17 of 44